AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior listings of claims in the application:

1. (currently amended): An electronic data storage system comprising:

a file device for storing at least electronic data; and

a data processing unit which

generates a first check ~~codes~~ code for detecting falsification ~~respectively for~~ of said electronic data and a second check code for detecting falsification of a public key-based electronic signature using a secret encryption method and/or an encryption key when the electronic data is registered,

stores said electronic data, said public key-based electronic signature, and said ~~respective~~ first and second check codes into said file device,

respectively verifies the validity of said stored electronic data and said electronic signature using said first and second check codes attached to the stored electronic data and said electronic signature when said electronic data is output, and then

accesses said electronic data and said electronic signature when said validity is confirmed,

wherein said data processing unit generates said first and second check codes by a method unique to said system, and

verifies the validity of said stored electronic data and said electronic signature by creating a third check code from said electronic data and a fourth check code from said electronic signature by said method unique to said system, and comparing said stored first check code with said third check code and said stored second check code with said fourth check code.

2. (currently amended): An electronic data storage system comprising:

a file device for storing at least electronic data; and

a data processing unit which

generates a check code for detecting falsification for a public key-based electronic signature using a secret encryption method and/or an encryption key when said electronic data is registered,

stores said electronic data, said public key-based electronic signature and the falsification check code for said electronic signature into said file device,

verifies the validity of said electronic signature using the check code attached to said electronic signature and

verifies the validity of said electronic data using said electronic signature when said electronic data is output, and then

accesses said electronic data and said electronic signature when said validity is confirmed,

wherein said data processing unit generates said check code by a method unique to said system, and

verifies the validity of said stored electronic data by creating a second check code from said electronic signature by said method unique to said system, and comparing said stored check code with said second check code.

3. (currently amended): The electronic data storage system according to Claim 1, wherein said data processing unit outputs said electronic data, ~~with attaching~~ the public key-based